ISSN No. 0976-5697

Volume 2, No. 3, May-June 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Applying Fuzzy logic and PGP to improve Security in Ad-hoc Network

V.Ramesh*
Research Scholar,
Sathyabama University
Chennai, India.
v2ramesh634@yahoo.co.in

N.Kotesar Rao
Assoc.Professor,
Dept.of IT, Narayana Engg College
Gudur, AP, India.
rao0007@gmail.com

Y.Neeraja
Associate Professor,
Dept of ECE, Narayana Engg College
Gudur, AP, India.
neerajareddy_31@yahoo.co.in

Abstract: In this paper, we study some latest developments on the topic of Mobile Ad hoc Network (MANET) Security. Among many developments, we think applying Fuzzy Logic algorithms and Pretty Good Privacy (PGP) security architecture to MANET security are novel and promising ideas. We look into these schemes in depth. We summarize and reiterate the main points in this paper. Further more, we analyze the weaknesses and drawbacks of proposed schemes, and propose our own improvements on base of the existing schemes.

Keywords— Mobile Ad-hoc Network, security, fuzzy logic, PGP

I. INTRODUCTION

Mobile ad hoc network (MANET) is a relatively new innovation in the field of wireless technology. These types of networks operate in the absence of fixed infrastructure, which makes them easy to deploy at any place and at any time. The absence of any fixed infrastructure in mobile ad hoc networks makes it difficult to adopt the existing techniques for network services, and poses a number of various challenges in the area.

Research on MANET security is still in its early stage. Various security mechanisms have been proposed, widely used, and proven to be effective in wired networks, but no single mechanism provides all the services required in a MANET. Due to certain characteristics of MANETs, some security mechanisms are not applicable to this environment. These certain characteristics of ad hoc networks include: lack of a network infrastructure and online administration, the dynamics of the network topology and node membership, the potential attacks from inside the network, and vulnerability of wireless links.

Existing proposals are typically attack-oriented in that they first identify several security threats and then enhance the existing protocol or propose a new protocol to thwart such threats. Different solutions have been proposed to address attacks in different layers. Because the solutions are designed explicitly with certain attack models in mind, they work well in the presence of designated attacks but may collapse under unanticipated attacks.

Many new schemes and proposals for ad hoc network security have come out in recent years. In this paper, we study some new developments on this topic: applying fuzzy logic algorithms and Pretty Good Privacy (PGP) to ad hoc network security. We first briefly introduce the author's idea, and analyse and propose our improvement on the author's idea.

II. APPLYING FUZZY LOGIC TO SECURE ROUTING PROTOCOLS

A. *Overview of Fuzzy Logic-based Security Level (FLSL) Routing Protocol.*

Nie et al [2] identify the critical problem of designing secure routing protocols in ad hoc networks. Based on traditional AODV and SAODV protocols, they propose to apply Fuzzy Logic algorithms in securing ad hoc network routing, and propose a new protocol – Fuzzy Logic-based Security Level (FLSL) Routing Protocol. The basic idea of FLSL is to utilize the "local multicast" mechanism and the Security-Level to select the highest Security-Level route. The proposed algorithm of Security-Level is an adaptive fuzzy logic based algorithm that can adapt itself with the dynamic conditions of mobile hosts.

Jin et al [3] studied the FLSL protocol and propose some improvement on FLSL. They suggest assigning a weight value to each entry in the rule set by taking the minimum of the three membership function values.

The authors state that most of secure routing protocols focus on the key management, authentication and encryption algorithm and these traditional routing protocols such as SAODV, SRP and SAR will fail to efficiently adapt to a higher security level routing selection, since the security level and selection of route are not part of their normal operation.

The new FLSL contains the way of determining the security-level of an individual mobile host in MANETs, and the algorithm to decide which route has the best security-level. In ad hoc networks, designing a secure routing protocol is critical. The FLSL routing protocol is proposed in [3].Authors described the characteristics and security management of the MANETs. An interesting property is that every node in the MANET has the field of Security-Level based on the fuzzy logic in the route tables to select the highest Security-Level route. The FLSL routing protocol can improve MANET's security. It is feasible to the weak security character of mobile ad hoc networks. The proposed algorithm of Security-Level is an adaptive fuzzy logic based algorithm that can adapt itself with the dynamic conditions of mobile hosts. Simulations show that the FLSL routing protocol can improve security of mobile ad hoc networks.

The basic idea of FLSL is that the FLSL routing protocol is a source-initiated on-demand routing protocol. It aims to find out the route with the highest Security-Level in the MANET. Because the Security-Level of a route is decided by the node which has the lowest Security-Level in that route, the node with the lowest Security-Level in the highest Security-Level route has higher security level than the node with the lowest Security-Level in other routes. In another word, the route with the highest Security-Level is comparably most secure.

The FLSL routing protocol is a source-initiated on-demand routing protocol, so nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges.

Inheriting from the AODV routing protocol, a node uses hello message that is periodic local broadcasts by a node to inform each mobile node in its neighborhood to maintain the local connectivity. A node should only use hello messages if it is part of an active route. Within the past delete period, it has received a hello message from a neighbor, and then for that neighbor does not receive any packets (hello messages or otherwise) for more than allowed_hello_loss* hello_interval milliseconds, the node should assume that the link to this neighbor is currently lost. When this happens, the node should send a route error (RERR) message to all precursors indicating which link is failed. Then the source initiates another route search process to find a new path to the destination or start the local repair.

FLSL protocol discovers and maintains only needed routes unlike traditional proactive protocols which maintain all routes regardless of their usage. In this protocol, the security-Level of a route is decided by the node which has the lowest Security-Level in that route. So compared with the lowest Security-Level in other routes, the lowest security level in the highest security level route is higher.

B. Factors Considered in Existing FLSL Protocol

So far, they have investigated three factors which are irrespective and independent with each other though, as follows:

a. Secret key length (l):

Longer the secret key is, stronger to defend serious brute force attack.

b. Changing Frequency of Secret Key (f):

If mobile host's secret key is changeable, the difficulty of decryption must be increased and security level of mobile hosts also gets enhanced.

c. Amount of Active Neighbour Hosts (n):

More active neighbour hosts existing will increase the percentage of potential attackers existing.

$$S \propto l \times f \times \frac{1}{n}$$

Based on these parameters, they define the security level (S) of a single mobile host. The relation between S and parameters is:

Use the given values of l, f and n to get corresponding fuzzy values from the member function figures basing on the fuzzy logic system rules table. These rules are basing on the observations and experiments.

For given input variables l, f, n, they have the membership degree values F(l), F(f), F(n). Then they assign a weight value to each entry in the rule set by taking the minimum of the three membership function values, *i*, associated with that entry. And for each *Wi* value, they calculate its corresponding *Si* value in the security level membership function figure.

After achieving the W_i and S_i values of each entries of rules table, the single mobile host's security level can be calculated by using:

$$SL_j = \frac{\sum_{i=1}^{12} W_i S_i}{\sum_{i=1}^{12} W_i} = \frac{W_1 S_1 + W_2 S_2 + \ldots + W_{12} S_{12}}{W_1 + W_2 + \ldots + W_{12}}$$

After the destination node received more than one RREQ packets, which means there are more than one available route, it will compare the security level values (SL_K) of the routes and select the most secure routes –max (SL_k) as the final route. The data packets from source node to destination node will be transmitted via this route.

The author conducted simulation experiment on their work using NS-2. Simulations show that the FLSL routing protocol can improve security of mobile ad hoc networks. They state that the simulation indicates that FLSL could reliably select the data transmission route with the highest security level and self-adaptive and dynamically adjust the route updating without delay. On the other hand, the simulation also shows that FLSL consumes more time for route discovery process. The authors analyse the time compensation and claim it is affordable and reasonable.

C. Our Improvement to FLSL

Having studied the existing schemes of FLSL, we notice there are some aspects to be improved. For one thing, the factors considered in the security level membership functions are not complete; more reasonable factors could be considered. For another thing, we think the weighted security level equation does not reflect the dynamic feature of nodes and communication links between nodes of MANETs. On ground of these thoughts, we propose to improve FLSL in the following ways:

a. Adding More Factors to Consideration

Security level-based routing protocols are not novel in ad hoc networks. The main contribution of the authors is to evaluate security level of a mobile node with fuzzy logic member functions and algorithms. This is a feasible solution. However, we think the fuzzy logic parameters considered in this scheme are not thorough and complete. We propose to add more factors to take into account.

For example, the following parameters can be added to the security level calculation:

Battery Indicator (b): A secure route should also be a reliable route. This requires all the nodes along this route have enough battery power.

Link-quality Indicator (q): In the original scheme, the number of active neighbour hosts is taken into account, but the quality of links to these neighbours is not. We suggest using a link-quality indicator parameter combined with the "number of active neighbours".

Having introduced the new parameters, the security level can be represented as:

$$S \propto l \times f \times b \times q \times \frac{1}{n} \times ......$$

We can define the fuzzy logic member functions for these new parameters, and calculate the weighted security level using:

$$SL_j = \frac{\sum_{i=1}^{12} W_i S_i}{\sum_{i=1}^{12} W_i} = \frac{W_1 S_1 + W_2 S_2 + ... + W_{12} S_{12}}{W_1 + W_2 + ... + W_{12}}$$

b. Weighted Moving Average of Security Level

We think the security level of a node is a time-variant system that changes over time. In this case, we suggest using weighted moving average of security level instead of a single time point value. The reasons for this are: First, in most systems there is fluctuation of security level. This may arise from the position of the moving node, the temporary interferences, and so on. The weighted moving average can filter off sharp fluctuation. Second, there is always some delay to get the latest value of security level and it is impossible to get the value in the next time point, while the weighted moving average provides a good estimation of the security level value in the future.

In our proposal, each node keeps a series of previous security level values: SL_n , SL_{n-1} , ……, SL_0 . The old, historical values need to be given lesser weight – or forgotten – in order to be able to estimate the latest value. This can be done by weighting the values as follows: For each value SL_i , we assign a weighted coefficient: $W_i = r^i$ *(r >1).* The weights wi are indexed so that w0 is the weight of the last value, w1 the second last, and so on.
The adjusted security level is:

$$SL = \frac{\sum_{i=0}^{n} W_i SL_{n-i}}{\sum_{i=0}^{n} W_i}$$

To reduce the memory requirement of the algorithm, we want to allow calculating SL without having to keep all the earlier samples in memory, by using the previous calculated result SL'. To this end, we update the estimate recursively as follows:

$$SL = \frac{1}{r} SL' + (1 - \frac{1}{r}) SL'$$

This is equivalent to using the exponential weights $W_i = r^i$ *(r >1),* since

$$SL = \frac{\sum_{i=0}^{n} W_i SL_{n-i}}{\sum_{i=0}^{n} W_i} = \frac{\sum_{i=0}^{n} r^{-i} SL_{n-i}}{\sum_{i=0}^{n} r^{-i}}$$

$$= \frac{SLi + \sum_{j=0}^{n-1} \frac{r^{-j}}{r} SL_{n-1-j}}{\sum_{i=0}^{n} r^{-i}} = \frac{SLi}{\sum_{i=0}^{n} r^{-i}} + \frac{1}{r} \frac{\sum_{j=0}^{n-1} \frac{r^{-j}}{r} SL_{n-1-j}}{\sum_{i=0}^{n-1} r^{-i} + r^{-n}}$$

$$\xrightarrow[n \to \infty]{} (1 - \frac{1}{r}) SL_i + \frac{1}{r} SL'$$

Letting zwe get $SL = \frac{n}{n+1} SL' + \frac{1}{n+1} SL_i$. This is a simplified equation to calculate the security level of a node that only needs keeping one historical data item.

III. APPLYING PGP TO BUILD A SELF-ADJUSTED SECURITY ARCHITECTURE

A. A Self Adjusted Security Architecture for Mobile Ad Hoc Networks

In [4], Ghalwash et al identify the problem of lack of security infrastructure and Certificate Authority (CA) service in mobile ad hoc networks. They propose self adjusted security architecture for ad hoc networks. Their work is based on Zimmermann's work of Pretty Good Privacy (PGP) [4], and merges the clustering and the threshold key techniques.

For any mobile ad hoc network to be secure and effective in the authentication (e.g. certificate-based authentication) operations a set of requirements needs to be satisfied:

a. Distributed authentication (e.g. in contrary to a fixed centralized central authentication CA in the network)
b. Resource awareness (e.g. relatively every operation in this distributed environment of nodes should take into consideration; power consumption and memory capacity)
c. Efficient certificate management mechanism (e.g. its not an easy task to control creation, revocation and renewal processes in a distributed MANET architecture)
d. Heterogeneous certification (e.g. There should be a clear hierarchy for the clusters to operates efficiently while distributing the certificates)
e. Robust pre-authentication mechanism (e.g. Having an earlier confidence level between the local nodes is an important step to avoid any further complication in the process of higher level of authentication)

Therefore, a decentralized certification authority approach has been taken in [5] using threshold cryptography and a network secret which to be distributed over a clustered network.

The method proposed is to partition the network into clusters and apply a complete certificate management system – public key system starting from the node variables assignment to the cluster head itself further to the central Authority, taking into consideration all the procedures that need to be addressed in the communication channel at each step.

They assigned four nodes to each cluster function as a part of the clustered authentication public key system (as shown in the figure below):

a. Cluster head: responsible for establishing and organizing the cluster.
b. Gateway nodes: managing communication between adjacent clusters
c. Warrant nodes
d. Regular nodes

There is an internal symmetric key for every cluster which is known to its members, it's used primarily to thwart eavesdropper by hiding the information in such an obfuscated method. Managing the key distribution among the cluster's head and nodes (releasing, renewing and scheduling) is done through an iterative process by assigning a secret share which is to be renewed regularly because the number of shares needs to be adapted to the number of cluster heads.

The public key of the cluster head network needs to be known to all nodes in the ad hoc network with additional status parameters about all nodes. For new node to enter a cluster (registration phase) it must pass through parametric negotiation between those nodes which have been assigned a trustworthy status by assigning a period of validity for the new node. Before that, the cluster head should check the validity of the trustworthy node itself before any action. And upon the condition of the new node (whether it's accepted in the cluster or not) the node will change to a guest node state after approving the Warrant Certificate procedures. What if a node wants to leave the cluster, additional steps needs to be taken to recalculate the new infrastructure status of the clustered network.

They also conducted a simulation experiment [4] using NS-2 to prove that their newly proposed architecture is more efficient in terms of time and availability (e.g. how long will it take for a node to achieve a granted status in the cluster). Register Time (the time period between receiving a cluster head beacon and acquiring a full membership in the cluster); is another proved factor in the simulation which shows the required time for a log-on (node) period to guarantee quick admissions of the mobile nodes to the ad hoc network.

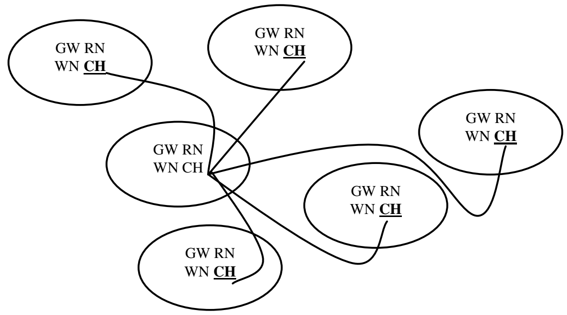

Figure 1

B. Weaknesses and Possible Improvements

While the dynamicity of MANETs topology (the architecture itself) creates a real need for security measurements and holistic implementation in a distributed environment, the overall security infrastructure is not sheltered enough to encompass such a highly promising technology. Hence, the proposal for distributed authentication is a good approach to alleviate the risk of the whole network being compromised. But this is not the issue, as the management in this case requires lots of additional constraints with multi dimensional agents to control the MANET clusters co-operations. Having said that, a certificate based approach as proposed by the author [4] to control the nodes inside the cluster is good somehow at some point but this is not always the case when it comes to large number of nodes (>>1000). Why, because the author tried to represent his theory graphically as a directed graph. While it is quite elegant to put the graph theory in practice in such a situation but the problem is the algorithm that needs to be used to parse each edge and node and to measure how efficient it is, in terms of efficiency, availability and complexity (space, time). As we know, for the graph there is a cost to traverse each edge associated with a capacity and flow variables.

The author did not mention in great depth about the implementation details of his proposed security architecture. It is almost theoretical, and the simulation results reflect only the time needed for the nodes clusters to start acquiring their allocated status dynamically (CH, Guest, GW) (security adaptation).

We propose an efficient mechanism for acquiring/releasing nodes existence by using a hash table which contains all the nodes required parameters to indicate their present/initial status. And this Hash Table should not be centralized in any way but partitioned and distributed over different clusters heads (as a special container). There is only one variable which indicated whether this node does it exist in this cluster or not. Therefore, this mechanism will just lessen the overhead in distributing the public/private keys over MANET clusters nodes.

Using a strong hash function like SHA-1 in the Hash Table is a must to avoid collision. The HT should be encrypted using public key system, and it has a tree structure like to manage all these nodes with their clusters. Actually, it is not easy to choose a balanced hash function which takes into account the computation and the time required to do a certain job because, simplicity, speed and strength are not a simple factors to combine them into a leveled scaled algorithm, especially in a MANET Network.

IV. DISCUSSIONS AND CONCLUSION

In this paper, we study some new ideas on MANET security published in last two years. Although these ideas are novel and promising, there exist some weaknesses and drawbacks in the proposed schemes which hinder the schemes to be applied generally. We propose some improvement on these ideas: for fuzzy logic security routing, we suggest using more factors to assess the security level of a node, and assessing the security dynamically by taking time weighted moving average; for PGP-based self-adjusted security architecture, we think the existing scheme is too resource-demanding and not scalable to large network; we propose to use some optimized data structure, such as hash table, to lower down the resource requirement.

Due to time limitation, we cannot implement our ideas for proof. However, by theoretical analysis, we believe if our proposals are employed in the original schemes, there would be significant improvement in the schemes.

V. REFERENCES

[1] D. Dhillon, T. Randhawa,M.Wang, L. Lamont, Implementing a fully distributed certificate authority in an OLSR MANET,WCNC 2004 IEEE Wireless Communication and Networking Conference, Atlanta, GA, USA, March 21−25, 2004.

[2] Jing Nie, JiangchuaWen, Ji Luo, Xin He, Zheng Zhou, An adaptive fuzzy logic based secure routing protocol in mobile ad hoc networks, Fuzzy Sets and Systems. pp1704-1712,2006.

[3] Lu Jin, Zhongwei Zhang and Hong Zhou, Deliberation and Implementation of Adaptive Fuzzy Logic Based Security Level Routing Protocol for Mobile Ad Hoc Network, Consumer Communications and Networking Conference, 2007

[4] AZ Ghalwash, AAA Youssif, SM Hashad, R Doss, 2007, Self Adjusted Security Architecture for Mobile Ad Hoc Networks, 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007) pp. 682-687

[5] P.Zimmermnn , "The Official PGP users guide", MIT Press, 1995

[6] A. Majlesi, B. H. Khalaj,AnAdaptive Fuzzy Logic Based Handoff Algorithm for Interworking betweenWLANS and Mobile Networks, PIMRC 2002.